SYSTEM AND METHODS FOR ANALYZING AND MODIFYING PASSWORDS

CROSS-REFERENCE TO RELATED APPLICATIONS

This nonprovisional application is a continuation of prior filed International Application PCT/US2012/062730 filed Oct. 31, 2012, and claims priority to provisional application No. 61/553,554, entitled "Password Analyzer and Modifier, and its Methods of Use and Production Thereof", filed by the same inventor on Oct. 31, 2011, which is incorporated herein by reference.

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

This invention was made with Government support under Grant No. 2006-DN-BX-K007 awarded by the National Institute of Justice. The government has certain rights in the invention.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to password analysis and modification. More specifically, it relates to analyzing password strength and developing strong passwords that are secure against efficient password cracking.

2. Description of the Prior Art

The use of passwords for protecting access is now ubiquitous in the Internet age, as Internet-based systems, such as online banking and online commerce, continue to rely heavily on passwords for authentication security. Human memorable passwords are thus a key element in the security of such systems. However, most users do not have the information to ensure that they are in fact using a "strong" password rather than one that can easily be broken. This limitation has led to the use and advocacy of password creation policies that purport to help the user in ensuring that the user chosen password is not easily breakable. The most prevalent password creation policy is the rule-based approach wherein users are given rules such as minimum length of eight characters and must contain an upper case letter and a special symbol. It has been shown by several authors that this approach by itself is not very effective (M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10); Oct. 4-8, 2010, pp. 163-175; E. R. Verheul, "Selecting secure passwords," M. Abe (Ed.): CT-RSA 2007, LNCS 4377, pp. 49-66, 2007). A second type of password creation policy can be termed the random approach where an effectively random string is given by a system to the user. Clearly, the random approach has the problem that the given string is generally non-memorable, so the purpose of having a password that can easily be remembered is defeated.

A strong password is one that is difficult to guess or crack, yet users continue to employ weak passwords that can often be easily guessed or broken by available password cracking systems. Existing technology is mostly based on giving advice to users on how to create a "secure password." Such advice is essentially a password creation policy, which advises users to follow rules while creating passwords. Suggested password creation rules include minimum length, use of upper case letters, lower case letters, and special symbols, including particular symbols. However, problems with these rules include inconsistencies within policies that are not based on a scientific approach, consequently resulting in a lack of strong passwords.

Moreover, current technologies tend to frustrate users when creating passwords because they do not allow users to utilize their normal password methods for choosing passwords. This leads to coping strategies, such as repeating a word just to make their passwords long enough to satisfy the policy requirements, which actually reduces password strength. Current restrictive policies are not user-friendly. These policies emphasize resistance to brute-force attacks, thus opening the password up to dictionary-based attack methods.

Existing technology also provides for password checkers that try to help users by providing a tool for them to check their password strength. These checkers propose to measure the strength of the proposed password based on certain parameters of the password. They check the password against some rules, give weights to the rules, and find an overall numeric value for the strength of the password. However, the rules used and weights given to the rules when applied to different parts of the proposed passwords are ad-hoc and have no scientific or empirical basis. These checkers do not define strength of a password based on evidence from real attacks, but define strength of a password generally based only on password structure, for example length of password, whether it can be found in the dictionary, etc.

Although not really an analysis of password strength, many studies attempt to determine various aspects of how users choose passwords. In Shannon Riley, "Password security: what users know and what they actually do," Usability News, 8(1), 2006, Riley reports that in a study of 315 participants, about 75% of them reported that they have a set of predetermined passwords that they use frequently. Almost 60% reported that they do not change the complexity of their password depending on the nature of the website they use. In B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: Analysis of a botnet takeover," Tech. Rep., April 2009, Stone-Gross et al. collected around 298 thousands passwords from the Torpig botnet. They found that almost 28% of users reused their passwords and they managed to crack over 40% of the passwords in less than 75 minutes. This illustrates that having strong passwords for less important websites such as social networking websites is likely to be as necessary as for websites such as online banking.

Most organizations and websites follow a rule-based approach in recommending or enforcing password policies. A study by Shay et al. (R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: user attitudes and behaviors," In 6th Symposium on Usable Privacy and Security, July 2010) showed that users were not happy about changing the password creation policy to a stricter one and that it took on average 1.77 tries to create a new password accepted by the system based on a new password creation policy recently instituted. Riley (Shannon Riley, "Password security: what users know and what they actually do," Usability News, 8(1), 2006) also reports that the average length of time users maintained their primary password was reported as 31 months and 52% of them never change their password at all.

Rule-based advice is confusing as there is no consistency across systems and websites in the requirements, with dif-